Outage Performance of Secure Multicasting in the Presence of Multiple Eavesdroppers

Jinxiao Zhu*‡, Yin Chen*, Yoshitaka Nakamura*, Xiaohong Jiang*‡, Osamu Takahashi*‡, and Norio Shiratori†
* School of Systems Information Science, Future University Hakodate, Japan.
† Prof. Norio Shiratori is with GITS, Waseda University, Tokyo and RIEC, Tohoku University, Sendai.
‡ Email: jxzhu1986@gmail.com, jiang@fun.ac.jp, osamu@fun.ac.jp.

***Abstract*—Recently, there has been a growing interest in applying multiple antennas to achieve information-theoretic security in wireless communication networks. In this paper, we consider the transmission of common confidential data from a single-antenna transmitter to multiple multi-antenna receivers in the presence of multiple multi-antenna eavesdroppers. Both the receivers and eavesdroppers employ maximal-ratio combining (MRC) to combine the signals received at multiple antennas. For the considered system, we derive its connection outage probability and secrecy outage probability to characterize the reliability level and the security level, respectively. Numerical results are also provided to analyze the tradeoff among the reliability and security performances and the number of antennas (or nodes) of either receivers or eavesdroppers.**

***Index Terms*—Physical layer security, secrecy outage probability, multiple antennas, multicast**

I. Introduction

Wireless multicasting, where a single stream of data is transmitted to multiple selected nodes simultaneously, has been an efficient and important method of supporting group communication [1]. Due to the inherent openness of wireless medium, the security of wireless multicasting has been a critical concern for these networks to support mission-critical applications, such as teleconferencing, mobile auctions, military command and control for tactical information.

Physical layer security, which achieves information-theoretic security by properly designing wiretap channel code according to the channel states [2], [3], has been demonstrated as a promising approach to providing strong secrecy for wireless networks. Pioneering works have been conducted to understand the performance of physical layer security, and a common conclusion from them is that perfect secrecy can be achieved when the quality of the channel from transmitter to legitimate receiver is better than that from transmitter to eavesdropper [2]–[4].

By now, many research works have been conducted for techniques to improve the performance of physical layer security, and these works can be roughly classified into three categories depending on where the technique is applied. Firstly, for techniques at the transmitter side, the works [5], [6] employed the multiple antennas to generate artificial noise such that the signal received at eavesdropper is considerably interfered while that at the target receiver has almost no interference. Transmit antenna selection scheme has been adopted in [7] to guarantee the channel quality of the targeted receiver. Interference alignment technique has been explored in [8] to achieve positive secure degrees of freedom. Secondly, for techniques at the receiver side, the multiple receive antennas have been adopted to mitigate fading effect and enhance channel quality [1], [9]. Thirdly, some techniques are implemented at neither transmitter nor receiver side, for example, cooperative jamming strategy at external helpers was studied in [10] to confuse the eavesdroppers.

This paper focuses on applying the multiple receive antennas to enhance the security of multicasting transmission based on physical layer security. In particular, we consider the scenario that both the legitimate receivers and eavesdroppers employ maximal ratio combining (MRC) reception scheme to combine the signals received by different antennas [11]. The main contributions of this paper are as follows.

- Under the assumption that the transmitter knows the real time channel state information (CSI) of the legitimate receiver channels but does not know that of the eavesdropper channels, we derive connection outage probability and secrecy outage probability in such a multicasting system with Rayleigh fading channel model. It is notable that the multicasting system model covers many other system models, e.g., the Rayleigh fading wiretap channel model in [12], and our theoretical results can be reduced to the result of the corresponding system model.
- Based on the above theoretical results, numerical results are provided to explore the tradeoff among the connection (or secrecy) outage probability and the number of antennas (or nodes) of either the legitimate receivers or the eavesdroppers.

The remainder of this paper is organized as follows. Section II presents system models and also introduces the performance metrics to analysis. In Section III, we derive the theoretical models of connection outage probability and secrecy outage probability. In Section IV, the impacts of system parameters on the outage probabilities are analyzed with numerical results. Finally, we conclude the paper in Section V.

II. System Model and Performance Metrics

Throughout the paper, the following notations will be used: Bold lower letters denote column vectors. A circularly symmetric complex Gaussian random variable x with variance σ^2 is denoted by $x \sim \mathcal{N}_{\mathbb{C}}(0, \sigma^2)$.

978-4-907626-12-9/15/$31.00 ©2015 IEEE

A. System Model

We consider a system where a transmitter multicasts its confidential data to L legitimate receivers in the presence of W eavesdroppers. The transmitter is equipped with one antenna while each of the legitimate receivers and eavesdroppers is equipped with N_R and N_E antennas, respectively. The communications are modeled as

$$\mathbf{y}_l(i) = \mathbf{h}_l(i)x(i) + \mathbf{n}_l(i), l = 1, 2, ..., L \quad (1)$$

$$\mathbf{z}_w(i) = \mathbf{g}_w(i)x(i) + \mathbf{n}_w(i), w = 1, 2, ..., W \quad (2)$$

where $i \in \{1, 2, ..., m\}$, m is the length of the channel input, $x(i)$ is the i-th channel input, $\mathbf{y}_l(i) \in \mathbb{C}^{N_R \times 1}$ and $\mathbf{z}_w(i) \in \mathbb{C}^{N_E \times 1}$ denote the signal vectors received by the corresponding legitimate receiver and eavesdropper, respectively, $\mathbf{h}_l(i) \in \mathbb{C}^{N_R \times 1}$ and $\mathbf{g}_w(i) \in \mathbb{C}^{N_E \times 1}$ are the respective channel gain vectors from the transmitter to the receiver and from the transmitter to the eavesdropper, and $\mathbf{n}_l(i)$, $\mathbf{n}_w(i)$ are AWGN vectors with i.i.d. entries following $\mathcal{N}_{\mathbb{C}}(0, \sigma_l^2)$ and $\mathcal{N}_{\mathbb{C}}(0, \sigma_w^2)$. We consider a quasi-static fading scenario where the channel gains, albeit random, are fixed during the transmission of an entire codeword, i.e., $\mathbf{h}_l(i) = \mathbf{h}_l$ and $\mathbf{g}_w(i) = \mathbf{g}_w$ for $\forall i$, and are independent from codeword to codeword. The entries of $\mathbf{h}_l$ and $\mathbf{g}_w$ are denoted by h_l^j and g_w^k, where $j \in \{1, 2, ..., N_R\}$ and $k \in \{1, 2, ..., N_E\}$. It is assumed that $h_l^j \sim \mathcal{N}_{\mathbb{C}}(0, \bar{H}_l)$ and $g_w^k \sim \mathcal{N}_{\mathbb{C}}(0, \bar{G}_w)$ for $\forall j$ and $\forall k$, i.e., the channels are subjected to Rayleigh fading.

We further assume that both the legitimate receivers and eavesdroppers know the instantaneous CSI (i.e., real time channel gains and phase shifts) of their own channels, and that the transmitter knows the instantaneous CSI of the legitimate receiver channels but does not know the instantaneous CSI of the eavesdropper channels. As such, both the legitimate receivers and eavesdroppers are assumed to apply MRC[1] reception scheme to combine the signals received by different antennas. It is also assumed that the eavesdroppers do not collude with each other[2], i.e., they process the received signals independently [14].

The transmitter has to satisfy a short-term average power constraint, P, for each codeword transmitted to the receivers. Consequently, the instantaneous SNR at the jth antenna of receiver l is given by

$$\gamma_l^j = P|h_l^j|^2/\sigma_l^2 \quad (3)$$

and its average value corresponds to

$$\bar{\gamma}_l = P\bar{H}_l/\sigma_l^2 \quad (4)$$

which is the same at all of the antennas of receiver l. Likewise, the instantaneous SNR at the kth antenna of eavesdropper w is given by

$$\gamma_w^k = P|g_w^k|^2/\sigma_w^2 \quad (5)$$

and its average value corresponds to

$$\bar{\gamma}_w = P\bar{G}_w/\sigma_w^2 \quad (6)$$

which is the same at all of the antennas of eavesdropper w. For the considered Rayleigh fading channel, γ_l^j and γ_w^k are exponential random variables with mean $\bar{\gamma}_l$ and $\bar{\gamma}_w$, respectively. Therefore, the combined SNRs γ_l and γ_w at the MRC outputs follow chi-square distribution and their respective probability density function (PDF) are given by [15]

$$f_{\gamma_l}(\gamma_l) = \frac{\gamma_l^{N_R-1}}{(N_R-1)!\bar{\gamma}_l^{N_R}} e^{-\gamma_l/\bar{\gamma}_l} \quad (7)$$

and

$$f_{\gamma_w}(\gamma_w) = \frac{\gamma_w^{N_E-1}}{(N_E-1)!\bar{\gamma}_w^{N_E}} e^{-\gamma_w/\bar{\gamma}_w}. \quad (8)$$

And their respective cumulative distribution function (CDF) are given by

$$F_{\gamma_l}(\gamma_l) = \frac{1}{(N_R-1)!}\zeta\left(N_R, \frac{\gamma_l}{\bar{\gamma}_l}\right) \quad (9)$$

and

$$F_{\gamma_w}(\gamma_w) = \frac{1}{(N_E-1)!}\zeta\left(N_E, \frac{\gamma_w}{\bar{\gamma}_w}\right), \quad (10)$$

where $\zeta(n, x) = \int_0^x t^{n-1}e^{-t}\mathrm{d}t$ is the lower incomplete gamma function.

B. Performance Metrics

In this paper, the physical layer security method[3] is adopted to ensure reliable and secure information transmissions in the concerned system. In this method, the transmitter needs to determine two rates, namely, the rate of the transmit codewords $\mathcal{R}_t$ and the rate of the confidential data $\mathcal{R}_s$. It is noticed that $\mathcal{R}_s \leq \mathcal{R}_t$, and the rate difference between the two rates, denoted by $\mathcal{R}_e = \mathcal{R}_t - \mathcal{R}_s$, indicates the rate cost of securing message transmissions against eavesdropping. For any transmitted message, a receiver is able to decode it with an arbitrary small error probability if $\mathcal{R}_t$ is *less* than the capacity of the channel from the transmitter to this receiver, while an eavesdropper is *not* expected to receive any information about the message if $\mathcal{R}_e$ is *larger* than the capacity of the channel from the transmitter to this eavesdropper.

In the above multicasting system, the design of transmission scheme should consider the receiver with the lowest SNR at the MRC outputs (denoted by $\gamma_{l(1)}$) and the eavesdropper with the highest SNR at the MRC outputs (denoted by $\gamma_{w(W)}$). A transmission is said to be reliable only when the codeword rate $\mathcal{R}_t$ is less than the receiver capacity determined by $\gamma_{l(1)}$, and security only only when $\mathcal{R}_e$ is larger than the eavesdropper capacity determined by $\gamma_{w(W)}$. As the instantaneous CSI of the legitimate receiver channels is available, the transmitter adopts an on-off transmission scheme, i.e., it transmits when $\gamma_{l(1)}$ exceeds some SNR threshold $\mu \geq 0$ and suspends the transmission otherwise. When transmits, $\mathcal{R}_t$ will be adaptively

[1]MRC reception has been regarded as the optimal diversity combining schemes as it maximizes the output SNR independent of the distributions of the branch signals [11], [13].

[2]If eavesdroppers collude with each other, they are at the risk of exposing themselves to the legitimate users.

[3]A detailed description about physical layer security method has been provided in [16].

set to the capacity determined by $\gamma_{l(1)}$, while $\mathcal{R}_s$ will be set a fix value. This is because the absence of real time CSI of eavesdropper channels at the transmitter sheds doubt on the operational significance of adopting a varying secrecy rate $\mathcal{R}_s$.

Based on the above transmission scheme, the reliability and security levels can be characterized by the following performance metrics, respectively.

- **Connection outage probability (COP)**: The connection outage probability, denoted by p_t, is defined as the probability that the lowest SNR $\gamma_{l(1)}$ at the MRC outputs of the legitimate receivers below the threshold μ:

$$p_t \triangleq \mathbb{P}\{\gamma_{l(1)} < \mu\}. \tag{11}$$

- **Secrecy outage probability (SOP)**: The secrecy outage probability, denoted by p_s, is defined as the probability that $\mathcal{R}_e$ less than the eavesdropper capacity determined by the highest SNR $\gamma_{w(W)}$ at the MRC outputs of the eavesdroppers during message transmissions:

$$p_s \triangleq \mathbb{P}\{\log(1+\gamma_{w(W)}) > \mathcal{R}_e | \gamma_{l(1)} \geq \mu\}. \tag{12}$$

Note that, in the above definition, the connection outage probability does not include the probability of outage events of $\{\log(1+\gamma_{l(1)}) < \mathcal{R}_t\}$ is due to the transmission scheme adopted in this paper. As described in [12], p_t can be interpreted as a quality of service (QoS) measure, while p_s measures the security level of the system.

III. Outage Performances

To derive the outage probabilities, we first need to determine the CDF of $\gamma_{l(1)}$ and $\gamma_{w(W)}$. Based on order statistics [17], the CDF of $\gamma_{l(1)}$ is given by

$$F_{\gamma_{l(1)}}(x) = 1 - [1 - F_{\gamma_l}(x)]^L \tag{13}$$

and the CDF of $\gamma_{w(W)}$ is given by

$$F_{\gamma_{w(W)}}(x) = [F_{\gamma_w}(x)]^W. \tag{14}$$

Replacing (10) into (14), the PDF of $\gamma_{w(W)}$ is then given by

$$f_{\gamma_{w(W)}}(x) = \frac{W}{(N_E-1)!}\frac{e^{-\frac{x}{\bar{\gamma}_w}}}{\bar{\gamma}_w}\left(\frac{x}{\bar{\gamma}_w}\right)^{N_E-1}\left(\frac{\zeta(N_E, \frac{x}{\bar{\gamma}_w})}{(N_E-1)!}\right)^{W-1}. \tag{15}$$

Regarding to the evaluation of p_t, we have the following theorem.

Theorem 1: In the concerned multicasting system where each of L receivers employs MRC to combine the signals received from its N_R antennas, the connection outage probability p_t for any given transmission SNR threshold $\mu \geq 0$ is given by

$$\begin{aligned} p_t &= F_{\gamma_{l(1)}}(\mu) \\ &= 1 - \left[1 - \frac{1}{(N_R-1)!}\zeta\left(N_R, \frac{\mu}{\bar{\gamma}_l}\right)\right]^L. \end{aligned} \tag{16}$$

Proof: The result can be directly derived by following by the definition of connection outage probability in (11). ■

Remark 1: When $N_R = L = 1$, (16) turns out to be the transmission outage probability under Rayleigh fading wiretap channel, which corresponds to Eq. (15) in [16].

From the above theoretical model of connection outage probability, it is noticed that p_t depends on the number of the legitimate receivers and the number of antennas on each receiver, and is independent of the number of the eavesdroppers and the number of antennas on each eavesdropper.

About the evaluation of secrecy outage probability p_s, we have the following theorem.

Theorem 2: In the concerned multicasting system with parameters N_R, N_E, L, W, $\bar{\gamma}_l$ and $\bar{\gamma}_w$ defined above, its secrecy outage probability p_s for any given transmission SNR threshold $\mu \geq 0$ and secrecy rate $R_s > 0$ is given in (17) on the top of the next page.

Proof: According to the definition of secrecy outage probability in (12) and the transmission scheme in Section II-B, we have

$$\begin{aligned} p_s &= \mathbb{P}\{\log(1+\gamma_{w(W)}) > \log(1+\gamma_{l(1)}) - \mathcal{R}_s | \gamma_{l(1)} \geq \mu\} \\ &= \mathbb{P}\{\gamma_{l(1)} < 2^{\mathcal{R}_s}(1+\gamma_{w(W)}) - 1 | \gamma_{l(1)} \geq \mu\} \\ &= \mathbb{P}\left\{\frac{\mu \leq \gamma_{l(1)} < 2^{\mathcal{R}_s}(1+\gamma_{w(W)}) - 1}{\gamma_{l(1)} \geq \mu}\right\} \\ &= \frac{1}{1-F_{\gamma_{l(1)}}(\mu)}\int_{\frac{\mu+1}{2^{\mathcal{R}_s}}-1}^{\infty} f_{\gamma_{w(W)}}(y)\int_{\mu}^{2^{\mathcal{R}_s}(1+y)-1} f_{\gamma_{l(1)}}(x)\mathrm{d}x\mathrm{d}y \\ &= 1 - F_{\gamma_{w(W)}}\left(\frac{\mu+1}{2^{\mathcal{R}_s}} - 1\right) - \frac{1}{1-F_{\gamma_{l(1)}}(\mu)} \\ &\quad \times \int_{\frac{\mu+1}{2^{\mathcal{R}_s}}-1}^{\infty} f_{\gamma_{w(W)}}(y)\left[1 - F_{\gamma_l}\left(2^{\mathcal{R}_s}(1+y) - 1\right)\right]^L \mathrm{d}y \end{aligned}$$

The final result in (17) can be derived by simplifying the above equation based on the following identities:

$$\Gamma(n, x) = \Gamma(n) - \zeta(n, x), \tag{18}$$

$$\zeta(n, x) = (n-1)!\left[1 - e^{-x}\sum_{j=0}^{n-1}\frac{x^j}{j!}\right], n = 1, 2, ... \tag{19}$$

and

$$(a+b)^n = \sum_{j=0}^{n-1}\binom{n}{j}a^{n-j}b^j. \tag{20}$$

■

Remark 2: When $N_R = N_E = L = W = 1$, (17) turns out to be the secrecy outage probability under Rayleigh fading wiretap channel, which corresponds to Eq. (7) in [12].

Based on the two outage probabilities in this paper, the (overall) outage probability that derived based on the outage definition in [4] can also be derived by following [16]

$$P_{out} = p_t + p_s(1 - p_t) \tag{21}$$

and setting $\mu = 2^{\mathcal{R}_s} - 1$. It is noticed that P_{out} corresponds to Eq. (14) in [1].

$$p_s = 1 - \left[F_{\gamma_w}\left(\frac{\mu+1}{2^{\mathcal{R}_s}} - 1\right)\right]^W - \frac{W}{[1-F_{\gamma_l}(\mu)]^L \bar{\gamma}_w^{N_E}(N_E-1)!} e^{-\frac{L}{\bar{\gamma}_l}\left[\left(2^{\mathcal{R}_s}-1\right)\right]} \sum_{i=0}^{W-1} \binom{W-1}{i} (-1)^i$$
$$\times \int_{\frac{\mu+1}{2^{\mathcal{R}_s}}-1}^{\infty} y^{N_E-1} e^{-\left(\frac{i+1}{\bar{\gamma}_w} + \frac{2^{\mathcal{R}_s}L}{\bar{\gamma}_l}\right)y} \left[\sum_{m=0}^{N_E-1} \frac{1}{m!}\left(\frac{y}{\bar{\gamma}_w}\right)^m\right]^i \left[\sum_{n=0}^{N_R-1} \frac{1}{n!}\left(\frac{1}{\bar{\gamma}_l}\left(\left(2^{\mathcal{R}_s}-1\right) + 2^{\mathcal{R}_s}y\right)\right)^n\right]^L \mathrm{d}y \qquad (17)$$

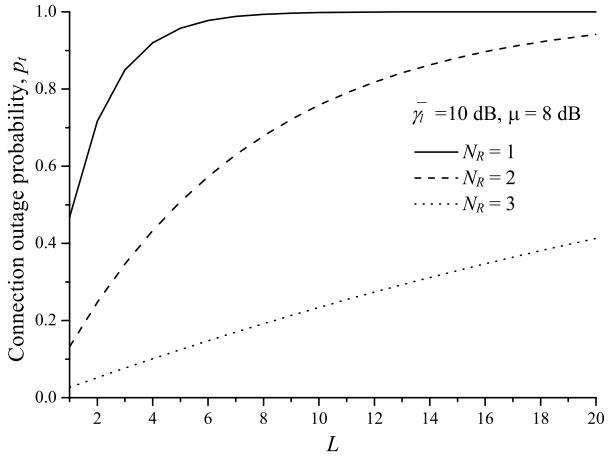

Fig. 1. Connection outage probability vs. the number of receivers L.

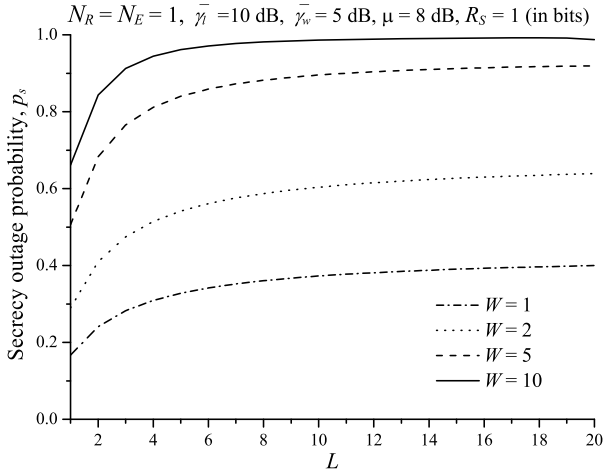

Fig. 2. Secrecy outage probability vs. the number of receivers L.

IV. Numerical Results and Discussions

Based on the theoretical models derived in this paper, this section illustrates the impact of system parameters on the reliability and security performances.

A. p_t vs. $\{L, N_R\}$

To illustrate the tradeoff between the reliability level and the number of the legitimate receivers (or the number of antennas on each receiver), we show in Fig. 1 how p_t varies with L for the scenarios of $\bar{\gamma}_l = 10$ dB, $\mu = 8$ dB and $N_R = \{1, 2, 3\}$. For all the three N_R scenarios, as shown in Fig. 1, p_t monotonically increases with L and approaches to 1 as L keeps increasing, which indicates that the reliability level will be deteriorated by increasing the number of legitimate receivers. This is due to the reason that the multicasting scheme needs to ensure the quality of the signal received at all targeted receivers, and that the probability of a worse channel becomes higher as the number of legitimate receivers L increases which results in a higher connection outage probability. We can also see from Fig. 1 that for a given L, a bigger N_R leads to a lower p_t. This indicates that the receiver's reliability level can be improved by increasing the number of antennas on each receiver.

B. p_s vs. $\{L, W\}$

To explore the tradeoff between the security level and the number of legitimate receivers (or eavesdroppers), we show in Fig. 2 how p_s varies with L for the scenarios of $N_R = N_E = 1$, $\bar{\gamma}_l = 10$ dB, $\bar{\gamma}_w = 5$ dB, $\mu = 8$ dB, $\mathcal{R}_s = 1$ (in bits) and $W = \{1, 2, 5, 10\}$. One can easily observe from Fig. 2 that p_s monotonically increases with L for all the four W scenarios, which indicates that the security level of the system is compromised when more legitimate receivers are targeted. One can further observe from Fig. 2 that for a given L, a bigger W leads to a higher p_s, which means that the security level decreases as the number of eavesdroppers increases.

C. p_s vs. $\{N_R, N_E\}$

To illustrate the tradeoff between the security level and the number of antennas on each legitimate receiver (or eavesdropper), we show in Fig. 3 how p_s varies with N_R for the scenarios of $L = W = 1$, $\bar{\gamma}_l = 10$ dB, $\bar{\gamma}_w = 5$ dB, $\mu = 8$ dB, $\mathcal{R}_s = 1$ (in bits) and $N_E = \{1, 5, 10, 20\}$. For all the four N_E scenarios, as shown in Fig. 3, p_s monotonically decreases with N_R, which indicates that the security level can be improved by increasing the number of antennas on each legitimate receiver. It is notable that p_s can be controlled to be arbitrary small by increasing N_R. For a given N_R, we can find in Fig. 3 that p_s becomes higher when N_E is larger, which shows that the security level drops down when the number of antennas on each eavesdropper increases.

D. p_s and P_{out}

We now make a comparison between the secrecy outage probability p_s (in (17)) and overall outage probability P_{out} (in (21)), two metrics used to illustrate the security level in the literature. For the case that $\mu = 2^{\mathcal{R}_s} - 1$, Fig. 4 illustrates how p_s and P_{out} vary with $\mathcal{R}_s$ for two different channel

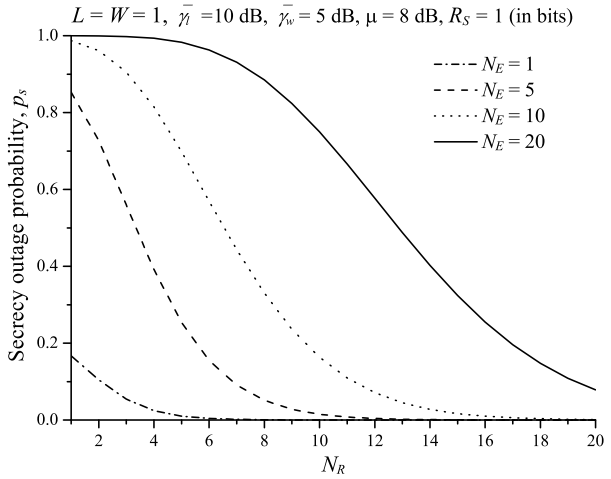

Fig. 3. Secrecy outage probability vs. the number of antennas on each receiver N_R.

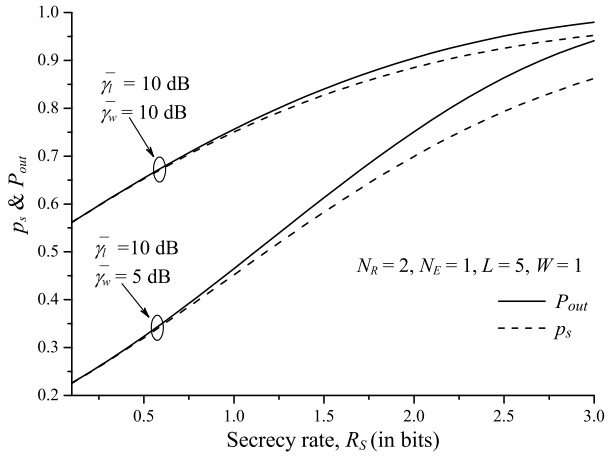

Fig. 4. Secrecy outage probability p_s and overall outage probability P_{out} vs. secrecy rate $\mathcal{R}_s$.

scenarios of $\bar{\gamma}_l$ and $\bar{\gamma}_w$: a normal scenario with $\bar{\gamma}_l = 10$ dB and $\bar{\gamma}_w = 10$ dB, and a better scenario with $\bar{\gamma}_l = 10$ dB and $\bar{\gamma}_w = 5$ dB. We can see from Fig. 4 that for all the two channel scenarios, P_{out} is larger than p_s, which indicates that using P_{out} in system design will result in a conservative estimation on $\mathcal{R}_s$. The above phenomenon is reasonable since P_{out} includes the probability of connection outage events and secrecy outage events.

V. Conclusion

This paper derived the theoretical models of connection outage probability and secrecy outage probability for the secure multicasting system where both the legitimate receivers and eavesdroppers are installed with multiple antennas. It is notable that our theoretical models, derived for multicasting system, also cover the corresponding results for other system models (e.g., the Rayleigh fading wiretap channel model) as special cases. The results in this paper indicate that the reliability and security performances can be improved by increasing the number of antennas on each legitimate receiver and will be deteriorated by increasing the other parameters (i.e., the number of legitimate receivers or eavesdroppers, and the number of antennas on each eavesdropper).

References

[1] A. P. Shrestha, J. Jung, and K. S. Kwak, "Secure wireless multicasting in presence of multiple eavesdroppers," in *13th Int. Symp. Commun. and Information Technologies (ISCIT)*, Sept. 2013, pp. 814–817.

[2] A. D. Wyner, "The wire-tap channel," *Bell System Technical Journal*, vol. 54, no. 8, pp. 1355–1387, 1975.

[3] S. K. Leung-Yan-Cheong and M. E. Hellman, "The gaussian wire-tap channel," *IEEE Trans. Inf. Theory*, vol. 24, no. 4, pp. 451–456, 1978.

[4] M. Bloch, J. Barros, M. R. D. Rodrigues, and S. W. McLaughlin, "Wireless information-theoretic security," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2515 – 2534, Jun. 2008.

[5] S. Goel and R. Negi, "Guaranteeing secrecy using artificial noise," *IEEE Trans. Wireless Commun.*, vol. 7, no. 6, pp. 2180–2189, 2008.

[6] X. Zhang, X. Zhou, and M. R. McKay, "Enhancing secrecy with multi-antenna transmission in wireless ad hoc networks," *IEEE Trans. Inf. Forensics Security*, vol. 8, no. 11, 2013.

[7] N. Yang, P. L. Yeoh, M. Elkashlan, R. Schober, and I. B. Collings, "Transmit antenna selection for security enhancement in mimo wiretap channels," *IEEE Trans. Commun.*, vol. 61, no. 1, pp. 144–154, 2013.

[8] O. O. Koyluoglu, H. El Gamal, L. Lai, and H. V. Poor, "Interference alignment for secrecy," *IEEE Trans. Inf. Theory*, vol. 57, no. 6, pp. 3323–3332, 2011.

[9] A. P. Shrestha and K. S. Kwak, "On maximal ratio diversity with weighting errors for physical layer security," *IEEE Commun. Lett.*, vol. 18, no. 4, pp. 580–583, 2014.

[10] J. Huang and A. L. Swindlehurst, "Cooperative jamming for secure communications in mimo relay networks," *IEEE Trans. Signal Processing*, vol. 59, no. 10, pp. 4871–4884, 2011.

[11] V. U. Prabhu and M. R. Rodrigues, "On wireless channels with m-antenna eavesdroppers: Characterization of the outage probability and ε-outage secrecy capacity," *IEEE Trans. Inf. Forensics Security*, vol. 6, no. 3, pp. 853–860, 2011.

[12] X. Zhou, M. R. McKay, B. Maham, and A. Hjørungnes, "Rethinking the secrecy outage formulation: A secure transmission design perspective," *IEEE Commun. Lett.*, vol. 15, no. 3, pp. 302–304, Mar. 2011.

[13] D. Brennan, "Linear diversity combining techniques," in *IRE*, vol. 47, no. 6, 1959, pp. 1075–1102.

[14] N. Romero-Zurita, M. Ghogho, and D. McLernon, "Outage probability based power distribution between data and artificial noise for physical layer security," *IEEE Signal Processing Letters*, vol. 19, no. 2, pp. 71–74, 2012.

[15] M. K. Simon and M.-S. Alouini, *Digital Communication over Fading Channels: A Uniform Approach to Performance Analysis*. John Wiley & Sons, 2000.

[16] J. Zhu, Y. Shen, X. Jiang, O. Takahashi, and N. Shiratori, "Secrecy capacity and outage performance of correlated fading wire-tap channel," *IEICE Trans. Commun.*, vol. E97-B, no. 2, pp. 396–407, Feb. 2014.

[17] H. A. David and H. Nagaraja, *Order Statistics*, 3rd ed. John Wiley & Sons, Inc., 2005.